From: ISS World Seminars
To: ndaigle@bakersfieldpd.us
Subject: Advanced Law Enforcement Training Seminars by Officers Mark Bentley and Chuck Cohen
Date: Sunday, February 26, 2017 3:09:14 PM

ISS World Training Seminars

Successful Use of Online Social Networking for Cyber Crime Investigation and Intelligence Gathering

April 6-7, 2017
London, UK

May 15-16, 2017
Miami, FL

Presented by:

Charles Cohen, **Cohen Training and Consulting, LLC** [Charles Cohen also holds the position of Commander, Cyber Crimes and Investigative Technologies Section, Indiana State Police

Complete Seminar Agenda and Registration

To review the full seminar agenda, or to register online, please click here or go to: www.issworldtraining.com

AGENDA

Advanced Cybercrime Investigators, Analysts and Digital Media Course

March 30-31, 2017
Washington, DC

April 4-5, 2017
London, UK

Presented by:

Mark Bentley, Former Child Exploitation and Online Exploitation (CEOP) Data comms Manager, UK National Crime Agency (NCA), and London Metropolitan Police. Full bio below description.

Complete Seminar Agenda and Registration

To review the full seminar agenda, or to register online, please click here or go to: www.issworldtraining.com

AGENDA

The content of this course is unique and

This two day (16 hour) course is designed for private and public sector investigators and analysts. Students with any level of familiarity with the Internet and computers, from beginning to advanced, will find this course beneficial.

The program gives students an up-to-date understanding of how social networking sites work and how members act and interact. Student will learn what information is available on various sites and how to integrate that information into criminal investigations and criminal intelligence analysis.

Session #1: Online Social Media: Tools, Tricks, and Techniques

Too often, investigators and analysts overlook or underutilize this valuable resource. Social networking sites are virtual communities. As in any large community, criminal organizations, fraud, violet crime, and victimization exist. Investigators need to understand these communities along with the tools, tricks, and techniques to prevent, track, and solve crimes.

Current trends include social networks based around live streaming video, like TinyChat and SnapChat, and mobile social networks like, Foursquare, Vibe, and Vine. These emergent technologies lead to risks and opportunities for law enforcement professionals that never previously existed. Current and future undercover officers must now face a world in which facial recognition and not available anywhere else. It will be supported by real world examples and incidents. This is not a general 'chalk and talk' course. It will teach you how to achieve results, and expand your thought process as to how. Law enforcement need to step up a gear and attack the growing threats face on.

The course will be a delivery / presentation / awareness format and is strictly restricted to Government and police as it contains new and innovative methodology and techniques.

The session descriptions below are specifically short, as a guide only. We are unable to openly publish the specifics of the techniques without alluding to the methods, which will remain clandestine, but will be fully explored during the sessions. New and innovative methods and techniques explained and shared, but will be up the individual forces and organisations to replicate the methods and procedures due to legal constraints.

COVERING:

- Advanced open source investigation
- OSINT tool website familiarisation
- Investigator tradecraft and good practice
- Dark web analysis and tracking
- Social Networking site interrogation and analytics
- Human anthropology Versus digital foot printing
- Social engineering tricks and exploits
- Financial and organisational security
- Tracking and identifying offenders, devices, footprints
- Temporal analysis of Hidden Web users

Internet caching make it possible to locate an online image posted years or decades before. The meshing of geolocation, metadata exploitation, social networking, and mobile devices allow officers to employ new investigative techniques not previously available.

Session #2: Facebook: Information Exploited

While there are over 1,000 social networking sites on the Internet, Facebook is by far the most populous, with over 1.1 billion profiles. It has a larger population as the US and UK combined, making it the third largest country by population. There are over 350 million images and 190 million status updates loaded on Facebook every day. This session will cover topics including Facebook security and account settings, Facebook data retention and interaction with law enforcement, and common fraud schemes involving Facebook. Recent additions and changes to Facebook, such as the Poke application for iOS devices, Graph Search, and Archive, make is more important than ever for investigators and analysts to fully understand this community.

Session #3: OSINT: Observation & Infiltration

Open source intelligence (OSINT) is a form of intelligence collection that involves finding, selecting, and acquiring information from publicly available

- Deep web analysis
- Exploits, injects and weaponising,
- Bitcoin tracking awareness
- Covert techniques and tricks.
- MAC, IMSI and IMEI evidential value and opportunities
- Device attribution

SESSION DESCRIPTION

The course will cover the following topics.

Investigator tradecraft and good practice
Just surfing the web doesn't evidentially hold up in court any more. In the real investigative world, we add layers of integrity and provenance to evidence, with property bags , statements and other supporting notes to get the evidence to court. Now we have to do the same virtually with online evidence and product. This session will show you good practice and watertight tradecraft in order to provide weighty and substantial evidence in court.

Advanced open source, lateral thinking and problem solving
"Sometimes, you have to stop looking for what you want to find, to find what you are looking for". This is one of my favourite, and most used phrases that sums this session up entirely. What else can we do that isn't obvious, to get where we want to get and identify the suspect? This session will show you how to specifically search data, look at non-obvious sources, analyse habit and human nature, and use it as a tool. Can you trust the data you're searching on? Are you searching all the ways to find data? This session will show you how to have good data hygiene and best practice, add integrity, and widening your virtual gaze.

Open source surfing and intel gathering

sources and then analyzing it to produce actionable intelligence. Now that the Internet is dominated by Online Social Media, OSINT is a critical component of both criminal and national security investigations. Too often, investigators and analysts overlook or underutilize this valuable resource.

Attendees will explore the challenges that analysts and investigators face differentiating between observation and infiltration of predicated chatter. The advantages and disadvantages of various methods to conceal identities while engaging in online observation and infiltration will be discussed.

Session #4: Counterintelligence & Liabilities Involving Online Social Media

Current and future undercover officers must now face a world in which facial recognition and Internet caching make it possible to locate an online image posted years or decades before. The meshing of geolocation, social networking, and mobile devices allow officers to employ new investigative techniques not previously available. There are risks posed to those in the public arena, and those charged with protecting them, associated with online social media and online social networking. The online social networking activities of employees, along with ever-increasing availability of information in the online public domain, present real challenges to companies and governments.

techniques and tools
There is a fine art and skill to open sourcing in the 21st Century. The investigator needs to know exactly how to 'talk' to search engines, to cut away the unnecessary digital flotsam which clouds the results, and get straight to the data required. This session will teach you to return results from search engines in manageable numbers of results - sometimes one page of data specifically and exactly what you were searching for. Just putting data into a search engine is a waste of time. Lets fine tune our requests and save time .

The lecturer runs an encrypted Law enforcement Open source tool site for investigators, based on 15 years of collection of useful tools. Delegates will be trained and familiarized with the 200+ OSINT tools therein, and provided with the password to use them.

Social Networking site interrogation and analytics
Social networking sites are great aren't they? Not from the perspective of the user - I mean that of the perspective of the investigator. We leave so much data on the web, it can lead to building up an extensive profile and leading us onto data we (and the suspect) didn't know they were leaving. Lets find it.

Human anthropology Versus digital foot printing
How we live, move and react with the real world is reflected in the digit footprint we leave in the virtual world. This session will look at where to look for clues in the data and footprint, to profile and help identify the person leaving it

Social engineering tricks and exploits
This session gives the delegate an understanding of the origins, impact and harm that the modern criminal social engineer plays in crime and intelligence security in the modern day internet. It covers both attack and defence. Can we

Session #5: What Investigators Need to Know about Hiding on the Internet

Criminal investigators and analysts need to understand how people conceal their identity on the Internet. Technology may be neutral, but the ability to hide ones identity and location on the Internet can be both a challenge and an opportunity. Various methods of hiding ones identity and location while engaged in activates on the Internet, provides an opportunity for investigators to engage in covert online research while also providing a means for criminals to engage in surreptitious communication in furtherance of nefarious activities. As technologies, such as digital device fingerprinting, emerge as ways to attribute identity this becomes a topic about which every investigator and analyst must become familiar.

Students receive course material, including legal process contact information, preservation letters, boilerplate compliance documents, and resource guides.

NOTICE: Course contains graphic content including profanity, and sexual and violent images.

ABOUT THE INSTRUCTOR

Chuck Cohen's formal education includes a Master of Business Administration from Indiana Wesleyan University and an undergraduate degree from Indiana University with a double major in Criminal Justice and

identify, exploit and copy their tactics?

Deep web analysis. "Googling it" doesn't cut the mustard any more. Its great for cheap flights and deals, but not for looking for people, digital shadows and historic footprints. Search engines can see less than a fifth of the Internet. Where else do we need to look? How can we look? What tools are there? Are we just looking at the big sites and should we look at the others? This session will take students deep into the Internet, and surprise many with what we will find, and can achieve, with an emphasis on the mind set, systematic approach and best practice methodology.

Injection and weaponising.
What can be weaponised or injected? How can we do it without detection? The advantages are self explanatory- but what are the pitfalls? What are the legal issues with this type of tracking? Can we do it and if so how?

Tracking Tor users and exploiting system vulnerabilities
Tor is a very difficult nut to crack. What if we stop looking at it and start looking at alternative vulnerabilities – and yes, even Tor has an Achilles heel. Lets have a look at it and start tracking users.

Temporal analysis and attribution. Are we thinking about everything when we track someone online? What sort of digital footprint are they leaving? Are we just looking at the obvious ones or are there some we don't know about? How can we find out? How do we cut away the giant virtual haystack of data to find the intelligence needle we were looking for? How can we track people successfully, who are adept at 'hiding' on the Internet? This session will show you how no one can hide. Attribution of a device to an individual is a major problem for Officers and prosecutors alike. This session will teach you good

Psychology. Chuck is also a Certified Fraud Examiner.

He is a Lieutenant serving the Indiana State Police, where he has been employed since 1994. He is currently the Commander, Cybercrime and Investigative Technologies Section. In this capacity, Lt. Cohen is responsible for the cybercrime, electronic surveillance, technical services, and Internet crimes against children units along with overseeing the department's overt and covert criminal intelligence function. Chuck is the Indiana Internet Crimes Against Children (ICAC) Task Force Commander.

Chuck speaks internationally on topics including the implications of online social networks in criminal investigations and criminal intelligence gathering, cybercrime, online fraud, money laundering, corruption investigations, and the investigation of skilled criminal offenders. He is an Adjunct Instructor at Indiana University Bloomington, where he teaches Foundations of Criminal Investigation.

Chuck was a member of the Office of the Director of National Intelligence Summer Hard Problem Program in 2008, 2009, and 2010. The 2008 the study topic was "3D Cyber Space Spillover: Where Virtual Worlds Get Real." The 2009 topic was "Mixed Reality: When Virtual Plus Real Equals One." And, in 2010, the topic was "Online Social Media."

practice to ensure there is sufficient data to prove attribution to an individual.

Attribution
A headache for most prosecutors and investigators. We can put a device at a location but how do we show who was there with the device.
What other clues are there to prove ownership and use? Let us look at them all.

MAC, IMSI and IMEI evidential value and opportunities
When we look at devices we focus on carrier, provider and capability. But what about The IMSI, MAC and IMEI? what can we do with these? How can we combat attempts by the user to tumble or mask them?

Advanced device tracking and digital non-visual surveillance.
Why does your smart phone battery die in less than a day? Its because it reaches out to the network 250,000 times an hour to allow you to have the very best experience from your provider. But where are these connections being made? Can the carrier see them? Can we see them and where can we find them? Never think ' there's no trace '. Have you ever had a case that went 'cold'? You will be re visiting it after this session.

Bitcoin tracking and exploits.
Have a bitcoin investigation? Can't track where the money went? In the real world, we can 'mark bills'. Can we do it with crypto currency? Let us see if we can track it…….

Covert techniques, profiles, identities, legends and tricks
Criminals and bad people play dirty and use dirty tricks. Can we play them at their own game? (Legally). Social engineering, scams, injection, ransomware? Let us brainstorm this and see…

Financial and organisational security

He is a published author, including peer-reviewed material and a cover article for Police Chief Magazine. Chuck was recently featured on the cover of the National White Collar Crime Center's Informant magazine and a feature guest on the syndicated radio program "The Badge" on SiriusXM. He was a subject matter expert for a Fox nationally syndicated show regarding criminal activity in online dating sites and for the Canadian Broadcasting Corporation's national news regarding criminal activity in Virtual Worlds.

Complete Seminar Agenda and Registration

To review the full seminar agenda, or to register online, please click here or go to: www.issworldtraining.com

Training for financial institutions and secure organisations re risks and attacks. The view point of the hacker and the would be thief and how that perception or targetting, of the banks Achilles heel , differs from that of the organisation or the IT within that business. Looking at both the attacking strategies and defensive work to future scan and defend against the as yet unseen threat. Live examples given . Also social engineering scams and defence.

NOTICE

Whilst every effort will be made to avoid, Due to the nature of the course, and live searching in the dark web, students may be exposed to disturbing or sexual images, profanity and graphic content, beyond the control of the presenter.

ABOUT THE INSTRUCTOR

Mark Bentley is a globally recognised communications data expert, who works as an adviser, trainer and consultant to security services, government and police forces around the world.

His experience is based on 35 years as a detective, which includes experience gained working for the UK National Crime Agency (NCA), Metropolitan police, and Child Exploitation and Online Exploitation (CEOP), in the capacity of overt, reactive and covert operations management.

He has been involved in the tracking of high profile cases, persons and vessels.

He is the Open source expert and lead advisor for forces and government agencies in several countries and advises on data analysis to government agencies, both domestic and abroad. Administrates and runs a leading , dedicated Law enforcement tools site for open sourcing.

His specialist area is device tracking and interrogation, alternative profile digital shadowing, injection and weaponising.

Mark presents this and other subjects to government and law enforcement around the world, both independently, and at ISS world training events. He is a lecturer for International policing organisations, EU cybercrime twinning project, The Council of Europe and The UK College of policing.

Complete Seminar Agenda and Registration

To review the full seminar agenda, or to register online, please click here or go to: www.issworldtraining.com

If you do not wish to receive future emails from ISS World Seminars, click here to opt-out.

TeleStrategies, Inc | 6845 Elm Street, Suite 310 | McLean | VA | 22101 | US